

AF TRW



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
Before the Board of Patent Appeals and Interferences

Applicant: A. M. Eskicioglu, et al.  
Ser. No.: 09/936,415  
Filed: September 12, 2001  
For: A GLOBAL COPY PROTECTION SYSTEM FOR DIGITAL HOME NETWORKS  
Examiner: Longbit Chai  
Art Unit: 2131

**APPEAL BRIEF**

May It Please The Honorable Board:

This is Appellants' Brief on Appeal from the final rejection of Claims 1-8, 10, 14 and 17-20, in support of the Notice of Appeal filed on May 22, 2006. Please charge the \$500.00 fee for filing this Brief to Deposit Account No. 07-0832. Appellants waive an Oral Hearing for this appeal.

Please charge any additional fee or credit overpayment to the above-indicated Deposit Account. Enclosed is a single copy of the Brief.

**I. REAL PARTY IN INTEREST**

The real party in interest of Application Serial No. 09/936,415 is the Assignee of record:

THOMSON (formerly THOMSON MULTIMEDIA)  
46 QUAI ALPHONSE LE GALLO  
F-92100 BOULOGNE BILLANCOURT, FRANCE

**II. RELATED APPEALS AND INTERFERENCES**

There are currently, and have been, no related Appeals or Interferences regarding the subject application known to the undersigned attorney.

08/23/2006 MWOLDGE1 00000045 070832 09936415

02 FC:1402

500.00 DA

\*\*\*\*\*

**Certificate of Mailing under 37 CFR 1.8**  
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in a postage paid envelope addressed to: Mail Stop: Appeal Briefs - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below.

Signature Lori Klewni

Date: Aug. 18, 2006

### **III. STATUS OF THE CLAIMS**

Claims 1-20 are rejected. The rejections of Claims 1-8, 10, 14 and 17-20 are appealed. Claims 9, 11-13, 15 and 16 have been cancelled, without prejudice, in the amendment filed contemporaneously herewith, a copy of which is attached hereto as Appendix IV.

### **IV. STATUS OF AMENDMENTS**

All prior amendments were entered. The claims included in Appendix I reflect each of the prior amendments, including the amendment filed contemporaneously herewith, a copy of which is attached hereto as Appendix IV.

### **V. SUMMARY OF CLAIMED SUBJECT MATTER**

This summary sets forth exemplary reference characters and pages and line numbers in the specification as originally filed where an embodiment of each separately argued claim is illustrated or described. The identification of reference characters and page and line numbers does not constitute a representation that any claim element is limited to the embodiment illustrated at the reference character or described in the referenced portion of the specification.

#### ***Claim 1***

Independent Claim 1 recites a method for managing access to a scrambled program, within a network comprising a first device interconnected to a second device. *See, e.g., Fig. 1A (access device 14 and presentation device 16); see also, page 4, lines 1-2 ("A global protection system for digital home networks, also known as extended conditional access, or XCA, is defined in this application.")*.

The method of Claim 1 includes (a) receiving said scrambled program in said first device, said scrambled program comprising a scrambled data component and a descrambling key. *See, e.g., page 6, lines 7-12 ("Content of economic value 11 whether from a tape, DVD, cable, satellite or terrestrial broadcast is usually delivered via a private conditional access service. The audio/video content and keys are protected and supplied to all the subscribers of the service using a private conditional access architecture. Subscribers who purchase content are supplied with the necessary keys for descrambling the content. Access device 14,*

*for example a set-top box, usually in conjunction with a smart card, obtains or generates the keys for descrambling the video content.”); see also, Fig. 1A (access device 14).*

The method of Claim 1 also includes (b) rebundling, in said first device, said descrambling key using a unique key associated with said first device. *See, e.g., page 12, lines 10-13 (“The keys for content descrambling are rebundled in LECMs by access device 14. That is, the encrypted ECMs, which carry the descrambling keys, are decrypted by access device 14 and then re-encrypted using a local public key associated with the access device to produce the LECM.”); see also, page 6, lines 21-22 (“(1) XCA Access Device 14 (e.g., set-top box, DVD player, DTV) creates “XCA protected content”); see also, Fig. 1A (access device 14).*

The method of Claim 1 also includes (c) receiving, in said second device, said scrambled data component and said rebundled descrambling key. *See, e.g., page 7, lines 15-18 (“The typical functions of an XCA device of Figure 2 are described below. The digital input 24 comprises all the circuitry and software needed to acquire a digital signal. The digital input may be of the form of a digital bus (e.g., IEEE 1394), a telco, a LAN, RF VSB/QAM or the like.”); see also, Fig. 1A (presentation device 16).*

The method of Claim 1 also includes (d) obtaining in said second device said descrambling key from said rebundled descrambling key. *See, e.g., page 13, lines 1-7 (“As shown in Figure 4, XCA protects the content on the local network by rebundling (i.e., ECM translation) 42 the keys required for descrambling (i.e., the TDES keys) into a new ECM which is protected by a local public key associated with the access device (i.e., LECM). This process is typically performed in access device 14 and preferably in security device 26. In this fashion, the only device capable of recovering the TDES keys and hence descrambling the MPEG program is the local presentation device, e.g., DTV.”); see also, Fig. 1A (presentation device 16).*

Finally, the method of Claim 1 includes (e) descrambling, in said second device, said scrambled data component using said descrambling key. *See, e.g., page 6, lines 22-23 (“(2) XCA Presentation Device 16 (e.g., DTV) descrambles “XCA protected content.”); see also, page 6, lines 30-32 (“Presentation devices, such as DTV 16, operate in combination with an XCA/NRSS Terminal Card (see 26b of Figure 5) for descrambling XCA protected content.”); see also, Fig. 1A (presentation device 16).*

**Claim 10**

Independent Claim 10 recites a method for managing access to a scrambled program received from a service provider within a network having an access device and a presentation device. *See, e.g., Fig. 1A (access device 14 and presentation device 16); see also, page 4, lines 1-2 (“A global protection system for digital home networks, also known as extended conditional access, or XCA, is defined in this application.”).*

The method of Claim 10 includes: (a) receiving said scrambled program in an access device, said scrambled program comprising a scrambled data component and an encrypted descrambling key. *See, e.g., page 6, lines 7-12 (“Content of economic value 11 whether from a tape, DVD, cable, satellite or terrestrial broadcast is usually delivered via a private conditional access service. The audio/video content and keys are protected and supplied to all the subscribers of the service using a private conditional access architecture. Subscribers who purchase content are supplied with the necessary keys for descrambling the content. Access device 14, for example a set-top box, usually in conjunction with a smart card, obtains or generates the keys for descrambling the video content.”); see also, Fig. 1A (access device 14).*

The method of Claim 10 also includes: (b) decrypting, in said access device, said encrypted descrambling key using a key associated with said service provider; and (c) re-encrypting said descrambling key, in said access device, using a public key associated with said access device. *See, e.g., page 12, lines 10-13 (“The keys for content descrambling are rebundled in LECMs by access device 14. That is, the encrypted ECMs, which carry the descrambling keys, are decrypted by access device 14 and then re-encrypted using a local public key associated with the access device to produce the LECM.”); see also, page 6, lines 21-22 (“(1) XCA Access Device 14 (e.g., set-top box, DVD player, DTV) creates “XCA protected content”); see also, Fig. 1A (access device 14).*

The method of Claim 10 also includes: (d) receiving, in said presentation device, said scrambled data component and said re-encrypted descrambling key. *See, e.g., page 7, lines 15-18 (“The typical functions of an XCA device of Figure 2 are described below. The digital input 24 comprises all the circuitry and software needed to acquire a digital signal. The digital input may be of the form of a digital bus (e.g., IEEE 1394), a telco, a LAN, RF VSB/QAM or the like.”); see also, Fig. 1A (presentation device 16).*

The method of Claim 10 also includes: (e) decrypting, in said presentation device, said re-encrypted descrambling key to obtain said descrambling key. *See, e.g., page 13, lines*

1-7 (*"As shown in Figure 4, XCA protects the content on the local network by rebundling (i.e., ECM translation) 42 the keys required for descrambling (i.e., the TDES keys) into a new ECM which is protected by a local public key associated with the access device (i.e., LECM). This process is typically performed in access device 14 and preferably in security device 26. In this fashion, the only device capable of recovering the TDES keys and hence descrambling the MPEG program is the local presentation device, e.g., DTV."*); see also, Fig. 1A (presentation device 16).

Finally, the method of Claim 10 includes: (f) descrambling, in said presentation device, said scrambled data component using said descrambling key. See again, page 13, lines 1-7 (*"As shown in Figure 4, XCA protects the content on the local network by rebundling (i.e., ECM translation) 42 the keys required for descrambling (i.e., the TDES keys) into a new ECM which is protected by a local public key associated with the access device (i.e., LECM). This process is typically performed in access device 14 and preferably in security device 26. In this fashion, the only device capable of recovering the TDES keys and hence descrambling the MPEG program is the local presentation device, e.g., DTV."*); see also, Fig. 1A (presentation device 16).

#### **Claim 17**

Independent Claim 17 recites an access device. See, e.g., Fig. 1A (access device 14). The access device of Claim 17 includes a signal input for receiving a scrambled program from a service provider, the scrambled program including a scrambled data component and an encrypted descrambling key. See, e.g., page 6, lines 7-12 (*"Content of economic value 11 whether from a tape, DVD, cable, satellite or terrestrial broadcast is usually delivered via a private conditional access service. The audio/video content and keys are protected and supplied to all the subscribers of the service using a private conditional access architecture. Subscribers who purchase content are supplied with the necessary keys for descrambling the content. Access device 14, for example a set-top box, usually in conjunction with a smart card, obtains or generates the keys for descrambling the video content."*); see also, Fig. 1A (access device 14); see also, Fig. 5 (access device 14 CA content input).

The access device of Claim 17 also includes a decrypting unit for obtaining the descrambling key using a key associated with the scrambled program. See, e.g., page 12, lines 10-13 (*"The keys for content descrambling are rebundled in LECMs by access device 14. That is, the encrypted ECMs, which carry the descrambling keys, are decrypted by*

*access device 14 and then re-encrypted using a local public key associated with the access device to produce the LECM.”); see also, page 6, lines 21-22 (“(1) XCA Access Device 14 (e.g., set-top box, DVD player, DTV) creates “XCA protected content”); see also, Fig. 1A (access device 14); see also, Fig. 5 (security device 26a CA module 42).*

The access device of Claim 17 also includes an encryption unit for re-encrypting the descrambling key using a public key associated with the access device. *See, e.g., page 12, lines 10-13 (“The keys for content descrambling are rebundled in LECMs by access device 14. That is, the encrypted ECMs, which carry the descrambling keys, are decrypted by access device 14 and then re-encrypted using a local public key associated with the access device to produce the LECM.”); see also, page 6, lines 21-22 (“(1) XCA Access Device 14 (e.g., set-top box, DVD player, DTV) creates “XCA protected content”); see also, Fig. 1A (access device 14); see also, Fig. 5 (security device 26a converter module 46).*

The access device of Claim 17 also includes a signal output coupled to a digital bus for transmitting the scrambled data component and the re-encrypted descrambling key to a presentation device via the digital bus, wherein only a presentation device having a corresponding private key is able to decrypt the re-encrypted descrambling key and descramble the scrambled content. *See again, page 13, lines 1-7 (“As shown in Figure 4, XCA protects the content on the local network by rebundling (i.e., ECM translation) 42 the keys required for descrambling (i.e., the TDES keys) into a new ECM which is protected by a local public key associated with the access device (i.e., LECM). This process is typically performed in access device 14 and preferably in security device 26. In this fashion, the only device capable of recovering the TDES keys and hence descrambling the MPEG program is the local presentation device, e.g., DTV.”); see also, Fig. 1A (presentation device 16); see also (Fig. 5, access device 14 CA/XCA content output).*

## **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Claims 1, 2, 5, 8 and 14 stand finally rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent No. 6,178,242 (hereinafter referred to as Tsuria). Claims 3, 6-7, 10, 17-18 and 20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria in view of United States Patent No. 5,870,474 (hereinafter referred to as “Wasilewski”. Claim 4 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria in view of United States Patent No. 5,481,609 (hereinafter referred to as Cohen).

Claim 19 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria, in view of Wasilewski, and further in view of United States Patent No. 5,948,136 (hereinafter referred to as Smyers).

## **VII. ARGUMENT**

### **Claims 1-8 & 14**

#### **A. Standard For Unpatentability Pursuant to 35 U.S.C. 102(e)**

A claim is anticipated pursuant to 35 U.S.C. 102 only if each and every element set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *See, Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). In other words, in order for a prior art reference to anticipate a claim, "the identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). And, each of the claim elements must be arranged as required by the claim. *See, In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990)

#### **B. Tsuria Fails to Disclose Each of the Limitations of Claim 1.**

Claim 1 recites:

A method for managing access to a scrambled program, within a network comprising a first device interconnected to a second device, the method comprising:

- (a) receiving said scrambled program in said first device, said scrambled program comprising a scrambled data component and a descrambling key;
- (b) rebundling, in said first device, said descrambling key using a unique key associated with said first device;
- (c) receiving, in said second device, said scrambled data component and said rebundled descrambling key;
- (d) obtaining in said second device said descrambling key from said rebundled descrambling key; and
- (e) descrambling, in said second device, said scrambled data component using said descrambling key.

Thus, Claim 1 calls for: (1) a first device to: (a) receive said scrambled program including a scrambled data component and a descrambling key; and (b) rebundle the descrambling key using a unique key associated with the first device; and (2) a second device to: (c) receive the scrambled data component and the rebundled descrambling key; (d) obtain the descrambling

key from the rebundled descrambling key; and (e) descramble the scrambled data component using the descrambling key. Tsuria fails to teach first and second devices performing these steps in such a manner (e.g., a first device performing steps (a)-(b) and a second device performing steps (c), (d) and (e)).

The appealed rejections argue Tsuria teaches a first device as IRD 110 and a second device as digital VCR 130. *See, 2/26/2006 Office action, par. 3, ll. 5-6.* The appealed rejections argue that the VCR 130 must be able to descramble a recording SDDS scrambled data component (SDSEG) using the TECM descrambling key or the system “can not work”. *See, 2/23/2006 Office action, pg. 3, ll. 4-6 (“Therefore, this second device must be able to descramble the scrambled data component using [a] descrambling key which is obtained from the rebundled descrambling key (i.e. TECM key).”), and 9-13 (“Examiner notes the similar operations similar to those performed on a broadcast SDDS is only the scrambling part of functions while the decoupling functions (i.e. descrambling) must be performed on the respective receiving device coupled to the first device – i.e. the second device is the digital VCR 130 playback device); otherwise, the system can not work properly (emphasis in original).”).* However, this misinterprets and misapplies the Tsuria teachings in a manner not supported by the reference itself, or in fact or logic.

As explained below, IRD 110 does not perform either step (d) obtaining in said second device said descrambling key from said rebundled descrambling key; or (e) descrambling, in said second device, said scrambled data component using said descrambling key. Instead, Tsuria squarely teaches IRD 110 performs all decrypting and descrambling functions.

In particular, Tsuria discloses an integrated receiver-decoder (IRD) 110 that receives a scrambled digital data stream (SDDS) from a broadcast source, the broadcast SDDS. *See, col. 7, ll. 34-35.* IRD 110 descrambles the broadcast SDDS using ECMs. *See, col. 7, ll. 48-57.* IRD 110 produces a recording SDDS and TECMs, where the TECMS are produced using keys similar to those of the ECMs. *See, col. 8, ll. 1-4, 17-28. 44-45.* Digital signals are sent between IRD 110 and VCR 130. *See, col. 7, ll. 30-32.* Playback of a recording SDDS from the digital VCR 130 is through IRD 110 to the television 100. *Col. 9, ll. 30-36.* During playback from VCR 130 through IRD 110, IRD 110 performs operations similar to those performed on a broadcast SDDS, but using the TECM key rather than the ECM key. *Col. 9, ll. 30-36.*

In other words, IRD 110 of Tsuria receives scrambled content, and descrambles it using ECMs. Thus, a clear signal corresponding to received scrambled content may be sent to television 100 by IRD 110. *See, annotated Fig. 1 (arrow between SDDS broadcast format and clear signal, reproduced and annotated below).*

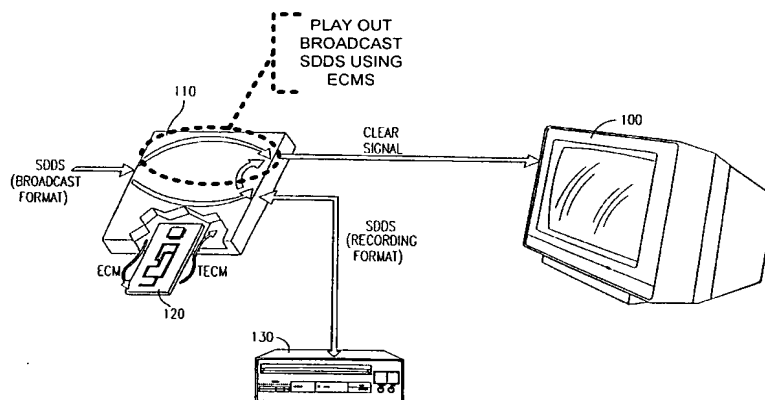


FIG. 1

IRD 110 of Tsuria also produces a recording SDDS from a received broadcast SDDS. In such a case the ECMs are essentially converted with TECMs, while the scrambled digital data segments (SDSEGs) remain encrypted. *See, e.g., col. 9, ll. 16-30; see also, Fig. 1 (arrow between SDDS broadcast format and SDDS recording format, reproduced and annotated below); see also, Fig. 2 (production of recording SDDS from broadcast SDDS, reproduced and annotated below).*

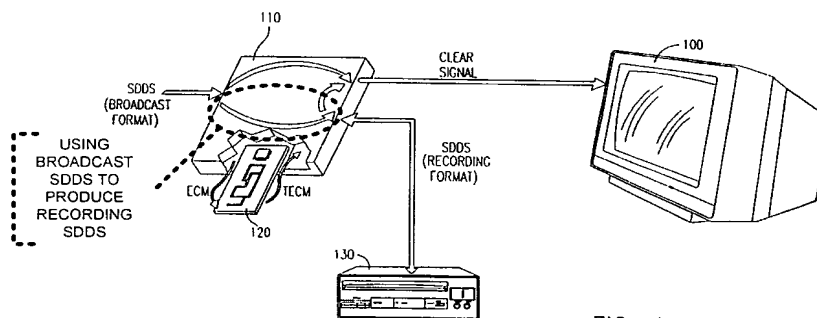
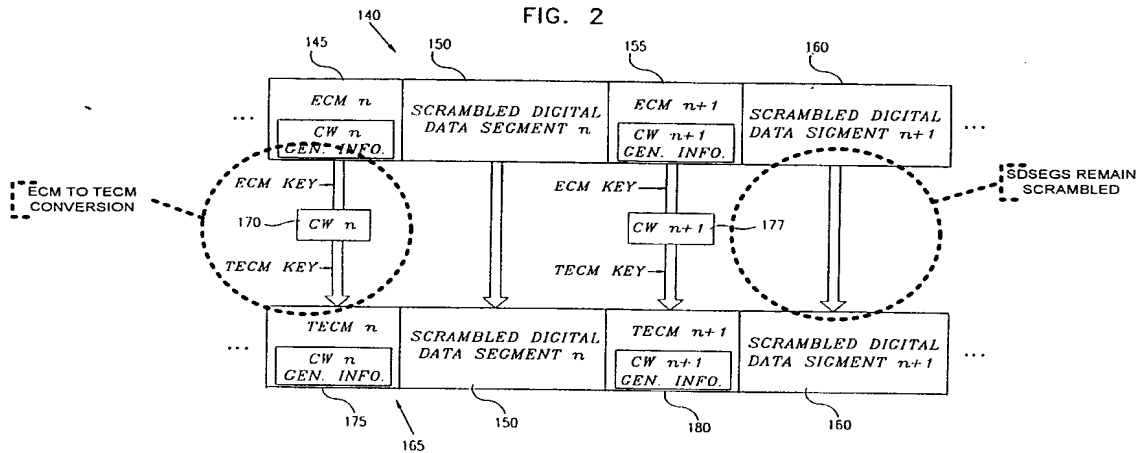
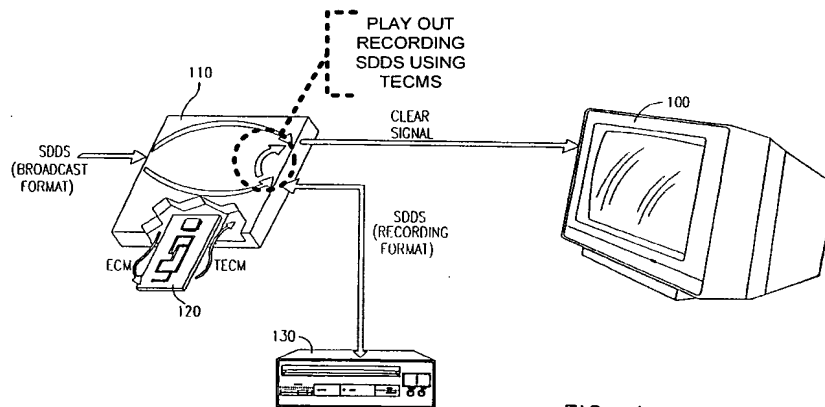


FIG. 1



Finally, a recording SDDS is played back from digital VCR 130 through IRD 110 to the television 100, such that IRD 110 and the associated smart card 120 (and not the VCR 130) perform descrambling operations using the TECM key. See, Col. 9, ll. 30-36; see also, Fig. 1 (arrow between recording SDDS and clear signal, reproduced and annotated below).



Tsuria discloses that IRD 110 accesses the TECMs and descrambles a recording SDDS. For example, Tsuria recites:

It is also appreciated that, during playback of a recording SDDS from the digital VCR 130 through the IRD 110 and associated smart card 120 to the television 100, the IRD 110 and the associated smart card 120 may perform operations similar to those performed on a broadcast SDDS, but using the TECM key rather than the ECM key. Col. 9, ll. 31-36 (emphasis added).

The appealed rejections argue these similar operations must equate only to scrambling and not descrambling. *See, 2/23/2006 Office action, page 3, ll. 9-11.* However, this is contrary to Tsuria's actual teachings. Appellant first notes there is no direct connection between VCR 130 and television 100 of Tsuria; playback of a recording SDDS is instead represented by the bi-directional arrow between IRD 110 and VCR 130.

Second, Tsuria explains that Fig. 3 (reproduced below) illustrates a block diagram of a portion of IRD 110. *See, col. 9, ll. 36-38.* Tsuria teaches, in connection with Fig. 3, that IRD 110 code word extractor 190 extracts code words from ECMs in the broadcast SDDS and provides them to IRD 110 descrambler 185. *See, col. 9, ll. 50-53.* IRD 110 descrambler 185 receives SDSEGs in the broadcast SDDS and applies the control words to the SDSEGs to produce a clear signal. *See, col. 9, ll. 53-56.*

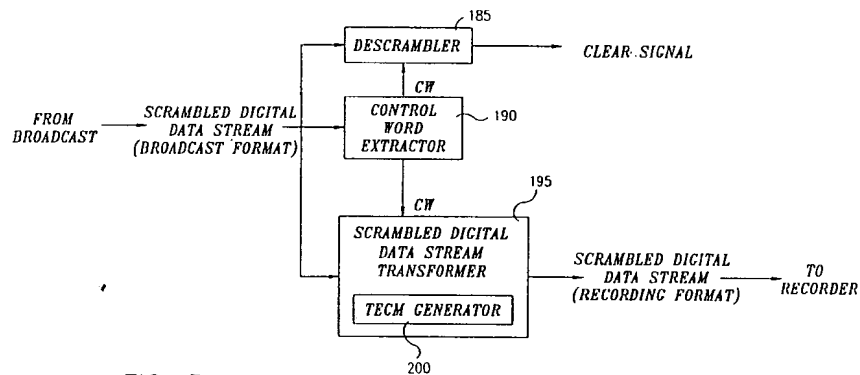


FIG. 3

Still further, Tsuria recites:

It is further appreciated that the [IRD 110] apparatus of FIG. 3 may be operative to descramble a recording SDDS and provide a clear signal therefrom by providing the recording SDDS as input to the apparatus of FIG. 3 in place of the broadcast SDDS, the control word extractor being operative in such a mode to provide control words, as described above, using a TECM key rather than an ECM key. Col. 10, ll. 10-16.

Thus, it is clear that whether a broadcast SDDS or a recording SDDS is being descrambled, Tsuria teaches that IRD 110 accesses (*e.g.*, extracts) control words using the ECM or TECM keys and actually descrambles the content – and not VCR 130.

In contradistinction to the speculation and unfounded assumptions used to support the appealed rejections, VCR 130 of Tsuria cannot be properly equated to the recited second device of Claim 1, as it fails to either “(d) obtain the descrambling key from the rebundled

descrambling key; [or] (e) descramble the scrambled data component using the descrambling key” – as the TECM is determined and the recording SDDS descrambled at IRD 110.

Accordingly, Tsuria fails to anticipate the system of Claim 1, as it fails to disclose, teach or suggest: (1) a first device to: (a) receive said scrambled program including a scrambled data component and a descrambling key; and (b) rebundle the descrambling key using a unique key associated with the first device; and (2) a second device to: (c) receive the scrambled data component and the rebundled descrambling key; (d) obtain the descrambling key from the rebundled descrambling key; and (e) descramble the scrambled data component using the descrambling key (*e.g.*, a first device performing steps (a)-(b) and a second device performing steps (c), (d) and (e)).

In view of the foregoing, Appellant requests reversal of the rejection of Claim 1 as being anticipated by Tsuria. Appellant also requests reversal of the rejections of Claims 2-8 and 14 as well, at least by virtue of these claims’ ultimate dependency upon a patentably distinct base Claim 1.

### Claim 10

#### **C. Standard For Unpatentability Pursuant to 35 U.S.C. 103(a)**

To establish a *prima facie* case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art. *See, MPEP 2143.03; see also, In re. Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)*. To establish a *prima facie* case of obviousness, there must also be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. *See, M.P.E.P. 706.02(j)*. Further yet, the teaching or suggestion to make the claimed combination must be found in the prior art, and not based on the applicant's own disclosure. *In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)*.

Further, each prior art reference must be considered in its entirety, *i.e.*, as a whole, including portions that would lead away from the claimed invention. *W.L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984)*. And, a *prima facie* case of obviousness can be rebutted where the cited art teaches away from the claimed invention in any material respect. *See, In re Haruna, 249 F.3d 1327, 58USPQ2d 1517 (Fed. Cir. 2001)*. A reference teaches away when a person of ordinary skill, upon reading the reference, would be led in a direction divergent

from the path that was taken by the applicant. *In re Haruna*, 249 F.3d 1327, 58USPQ2d 1517.

**D. Tsuria and Wasilewski Fail to Render Claim 10 Unpatentable, As Tsuria And Wasilewski Fail To Teach Or Suggest Each Of The Limitations Of Claim 10.**

Claim 10 recites:

A method for managing access to a scrambled program received from a service provider within a network having an access device and a presentation device, said method comprising:

- (a) receiving said scrambled program in an access device, said scrambled program comprising a scrambled data component and an encrypted descrambling key;
- (b) decrypting, in said access device, said encrypted descrambling key using a key associated with said service provider;
- (c) re-encrypting said descrambling key, in said access device, using a public key associated with said access device;
- (d) receiving, in said presentation device, said scrambled data component and said re-encrypted descrambling key;
- (e) decrypting, in said presentation device, said re-encrypted descrambling key to obtain said descrambling key; and
- (f) descrambling, in said presentation device, said scrambled data component using said descrambling key.

In similar fashion to Claim 1 discussed above, Claim 10 calls for first and second devices, in that it recites an access device to: (a) receive scrambled program content, (b) decrypt a descrambling key; and (c) re-encrypt the descrambling key; and a presentation device to: (d) receive the scrambled data and re-encrypted key; (e) decrypt the re-encrypted key; and (f) descramble the content.

Like Claim 1, the appealed rejection of Claim 10 relies upon Tsuria as teaching recited steps (e) and (f) being performed in a presentation device (*e.g.*, a second device or VCR 130) -- (e) decrypting, in said presentation device, said re-encrypted descrambling key to obtain said descrambling key; and (f) descrambling, in said presentation device, said scrambled data component using said descrambling key. *See*, 2/23/2006 Office action, pg. 10, ll. 18-21. Again, in contradistinction to the speculation and unfounded assumptions used to support the appealed rejections, VCR 130 of Tsuria cannot be properly equated to the

recited presentation device of Claim 1, as it fails to either: (e) decrypt said re-encrypted descrambling key to obtain said descrambling key; or (f) descramble said scrambled data component using said descrambling key. Rather, as discussed above, IRD 110 of Tsuria accesses (*e.g.*, extracts) control words using the ECM or TECM keys and actually descrambles the content – and not VCR 130.

Wasilewski is not relied upon in the appealed rejection of Claim 10 to remedy either of these deficiencies of Tsuria – and is instead merely relied upon for its purported teachings regarding public key cryptography. *See, 2/23/2006 Office action, pg. 11, ll. 3-7.* Accordingly, a *prima facie* case of obviousness with respect to Claim 10 has not been presented.

Wherefore, Appellant requests reversal of the rejection of Claim 10 as being unpatentable over Tsuria in view of Wasilewski.

#### **Claims 17-20**

#### **E. Tsuria and Wasilewski Fail to Render Claim 17 Unpatentable, As Tsuria And Wasilewski Fail To Teach Or Suggest Each Of The Limitations Of Claim 17.**

Claim 17 recites:

An access device, comprising:  
a signal input for receiving a scrambled program from a service provider, the scrambled program including a scrambled data component and an encrypted descrambling key;  
a decrypting unit for obtaining the descrambling key using a key associated with the scrambled program;  
an encryption unit for re-encrypting the descrambling key using a public key associated with the access device;  
a signal output coupled to a digital bus for transmitting the scrambled data component and the re-encrypted descrambling key to a presentation device via the digital bus, wherein only a presentation device having a corresponding private key is able to decrypt the re-encrypted descrambling key and descramble the scrambled content.

Claim 17 calls for an access device that has: (a) an input that receives a scrambled data component and a descrambling key; (b) a decrypting unit that obtains the descrambling key; (c) an encryption unit that re-encrypts the descrambling key; and (d) an output coupled to a digital bus. Claim 17 further recites that only a presentation device having a corresponding private key is able to decrypt the re-encrypted descrambling key and descramble the scrambled content.

The appealed rejections rely upon Wasilewski only for its purported teachings regarding public key cryptography. *See, 2/23/2006 Office action, pg. 14, ll. 10-12* (“*Wasilewski teaches using the public key as the higher-level encryption key to protect the lower-level encryption key over a communications network to the receiving terminal module.*”); *see also, 2/23/2006 Office action, pg. 15, ll. 3-4* (“*Wasilewski: Column 3 Line 62-65 & Tsuria: see the same rationale of response to arguments as stated above in the claim 1*”).

Tsuria does not teach, or even suggest, that VCR 130 can decrypt re-encrypted descrambling keys or descramble content – let alone that only VCR 130 can decrypt re-encrypted descrambling keys and descramble content. To the contrary, and as described above, Tsuria teaches IRD 110, the same device that decrypts the encrypted scrambling key and re-encrypts the descrambling key, is the only device that can decrypt the re-encrypted descrambling key. *See, e.g., col. 8, ll. 38-45* (“*The use of such a digital signature is considered preferable in order to discourage unauthorized duplication and subsequent playback of the recording SDDS 165 using apparatus other than the apparatus of FIG. 1, particularly using a different smart card at some other location in place of the smart card 120.*”, where smart card 120 is coupled to IRD 110 (*see, Fig. 1*)).

Accordingly, Tsuria and Wasilewski fail, in any combination, to teach or suggest an access device that includes: (a) an input that receives a scrambled data component and a descrambling key; (b) a decrypting unit that obtains the descrambling key; (c) an encryption unit that re-encrypts the descrambling key; and (d) an output coupled to a digital bus, wherein only a presentation device having a corresponding private key is able to decrypt the re-encrypted descrambling key and descramble the scrambled content.

Accordingly, a *prima facie* case of obviousness with respect to Claim 17 has not been presented. Wherefore, Appellant requests reversal of the rejection of Claim 17 as being unpatentable over Tsuria in view of Wasilewski. Appellant also requests reversal of the rejections of Claims 18-20 as well, at least by virtue of these claims’ ultimate dependency upon a patentably distinct base Claim 17.

**F. No Proper Motivation Exists For Modifying The Primary Reference (Tsuria) To Only Enable A Device Distinct From the Access Device To Decrypt Re-Encrypted Descrambling Keys, As Recited by Claim 17**

As discussed above, Tsuria teaches that IRD 110, the same device that decrypts the encrypted scrambling key and re-encrypts the descrambling key is the only device that can decrypt the re-encrypted descrambling key. *See, e.g., col. 8, ll. 38-45* (“*The use of such a digital signature is considered preferable in order to discourage unauthorized duplication and subsequent playback of the recording SDDS 165 using apparatus other than the apparatus of FIG. 1, particularly using a different smart card at some other location in place of the smart card 120*”, where smart card 120 is coupled to IRD 110 (see, Fig. 1)).

Thus, Tsuria teaches away from the recited invention of Claim 17, which recites that only a presentation device distinct from the access device that decrypts the encrypted scrambling key and re-encrypts the descrambling key can decrypt the re-encrypted descrambling key. In other words, Tsuria would lead a skilled artisan in a direction divergent from that path recited in Claim 17, as Tsuria instead teaches that a same access device (IRD 110) should be used for both re-encrypting the scrambling key and decrypting the re-encrypted scrambling key.

Accordingly, no motivation exists for modifying Tsuria to enable only a presentation device distinct from the access device that decrypts the encrypted scrambling key and re-encrypts the descrambling key to decrypt the re-encrypted descrambling key, in direct contradiction to Tsuria’s teaching that a same access device (IRD 110) should be used for both re-encrypting the scrambling key and decrypting the re-encrypted scrambling key, absent impermissible hindsight gleaned from Applicant’s own disclosure.

**G. Conclusion**

Reversal of all appealed rejections is therefore requested, at least by reason that: (1) Tsuria fails to teach each of the limitations of any of Claims 1, 2-8 and 14; (2) Tsuria and Wasilewski fail, in any combination, to teach each of the recited limitations of any of Claims 10 and 17-20; and (3) a proper motivation for modifying Tsuria to enable only a presentation device distinct from the access device that decrypts the encrypted scrambling key and re-encrypts the descrambling key to decrypt the re-encrypted descrambling key, in direct contradiction to Tsuria's teaching that a same access device (IRD 110) should be used for both re-encrypting the scrambling key and decrypting the re-encrypted scrambling key, is lacking.

Respectfully submitted,

A: M. Eskicioglu et al.

By:



Paul Kiel, Attorney  
Registration No. 41,736  
(609) 734-6807

Patent Operations  
Thomson Licensing Inc.  
P.O. Box 5312  
Princeton, NJ 08543-5312  
August 18, 2006

**APPENDIX I - APPEALED CLAIMS**

1. (Previously Presented) A method for managing access to a scrambled program, within a network comprising a first device interconnected to a second device, the method comprising:
  - (a) receiving said scrambled program in said first device, said scrambled program comprising a scrambled data component and a descrambling key;
  - (b) rebundling, in said first device, said descrambling key using a unique key associated with said first device;
  - (c) receiving, in said second device, said scrambled data component and said rebundled descrambling key;
  - (d) obtaining in said second device said descrambling key from said rebundled descrambling key; and
  - (e) descrambling, in said second device, said scrambled data component using said descrambling key.
2. (Previously Presented) The method of Claim 1 wherein said descrambling key is encrypted and the step of rebundling comprises:
  - (a) decrypting said encrypted descrambling key using a key associated with said scrambled program; and
  - (b) re-encrypting said descrambling key using said unique key associated with said first device to produce said rebundled descrambling key.
3. (Previously Presented) The method of Claim 2 wherein said unique key associated with said first device is a public key, said public key being located in said first device and a corresponding private key being located in said second device.
4. (Previously Presented) The method of Claim 2 wherein the step of rebundling is performed within a first smart card coupled to said first device and the steps of obtaining and descrambling are performed within a second smart card coupled to said second device.
5. (Original) The method of Claim 1 further comprising the step of initializing said first device within said network.

6. (Previously Presented) The method of Claim 5 wherein the step of initializing comprises the step of receiving a public key from a conditional access provider, said step of receiving comprising authentication of said conditional access provider.
7. (Previously Presented) The method of Claim 5 wherein a public key is prestored in a smart card coupled to said first device or in said first device.
8. (Previously Presented) The method of Claim 1 wherein said descrambling key is encrypted using a private means if said scrambled program is received from pre-recorded media or protected by a private means if said scrambled program is received from a service provider.
9. (Cancelled)
10. (Previously Presented) A method for managing access to a scrambled program received from a service provider within a network having an access device and a presentation device, said method comprising:
  - (a) receiving said scrambled program in an access device, said scrambled program comprising a scrambled data component and an encrypted descrambling key;
  - (b) decrypting, in said access device, said encrypted descrambling key using a key associated with said service provider;
  - (c) re-encrypting said descrambling key, in said access device, using a public key associated with said access device;
  - (d) receiving, in said presentation device, said scrambled data component and said re-encrypted descrambling key;
  - (e) decrypting, in said presentation device, said re-encrypted descrambling key to obtain said descrambling key; and
  - (f) descrambling, in said presentation device, said scrambled data component using said descrambling key.
11. (Cancelled)

12. (Cancelled)
13. (Cancelled)
14. (Original) The method of claim 1, wherein the first device is an access device and wherein the second device is a presentation device.
15. (Cancelled)
16. (Cancelled)
17. (Previously Presented) An access device, comprising:
  - a signal input for receiving a scrambled program from a service provider, the scrambled program including a scrambled data component and an encrypted descrambling key;
  - a decrypting unit for obtaining the descrambling key using a key associated with the scrambled program;
  - an encryption unit for re-encrypting the descrambling key using a public key associated with the access device;
  - a signal output coupled to a digital bus for transmitting the scrambled data component and the re-encrypted descrambling key to a presentation device via the digital bus, wherein only a presentation device having a corresponding private key is able to decrypt the re-encrypted descrambling key and descramble the scrambled content.
18. (Previously Presented) The access device of claim 17, wherein the public key is periodically received from a conditional access provider.
19. (Previously Presented) The access device of claim 17, wherein the signal output authenticates the presentation device before transmitting the scrambled data component and the re-encrypted descrambling key to the presentation device.

20. (Previously Presented) The access device of claim 17, wherein the signal output transmits identification data associated with the access device and copy control information along with the re-encrypted descrambling key.

**APPENDIX II - TABLE OF CASES**

<i>Verdegaal Bros. v. Union Oil Co. of California</i> , 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)	7
<i>Richardson v. Suzuki Motor Co.</i> , 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)	7
<i>In re Bond</i> , 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990)	7
<i>W.L. Gore &amp; Associates, Inc. v. Garlock, Inc.</i> , 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984)	12
<i>In re. Royka</i> , 490 F.2d 981, 180 USPQ 580 (CCPA 1974)	12
<i>In re Vaeck</i> , 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)	12
<i>In re Haruna</i> , 249 F.3d 1327, 58USPQ2d 1517 (Fed. Cir. 2001)	12

**APPENDIX III - LIST OF REFERENCES**

<b><u>U.S. Pat. No.</u></b>	<b><u>Issued Date</u></b>	<b><u>102(e) Date</u></b>	<b><u>Inventors</u></b>
6,178,242	01/23/2006	01/28/1998	Yossef Tsuria
5,481,609	01/02/1996	09/10/1993	Michael Cohen
5,948,136	09/07/1999	07/30/1997	Scott D. Smyers
5,870,474	02/09/1999	12/29/1995	Anthony John Wasilewski

CUSTOMER NO. 24498  
Serial No.: 09/936,415

RCA89462

**APPENDIX IV – AMENDMENT AFTER NOTICE OF APPEAL**

TABLE OF CONTENTS

I.	Real Party in Interest	1
II.	Related Appeals and Interferences	2
III.	Status of Claims	2
IV.	Status of Amendments	2
V.	Summary of Claimed Subject Matter	2-5
VI.	Grounds of Rejection to be Reviewed on Appeal	6
VII.	Argument	7-16
VIII	Conclusion	17

APPENDICES

I.	Appealed Claims	18-21
----	-----------------	-------

II.	Table of Cases	22
III.	List of References	23
IV.	Amendment	24